Title
The Syllabus as a Student Privacy Document in an Age of Learning Analytics

Authorship
Kyle M. L. Jones
Indiana University–Indianapolis (IUPUI)
School of Informatics and Computing, Department of Library and Information Science
kmlj@iupui.edu

Amy VanScoy
University at Buffalo
Graduate School of Education, Department Information Science
vanscoy@buffalo.edu

Correspondence
All correspondence should be directed to Dr. Jones via e-mail at kmlj@iupui.edu or kylejones@thecorkboard.org.

This is the author's manuscript of the article published in final edited form as:

Jones, K. M. L., & VanScoy, A. (2019). The syllabus as a student privacy document in an age of learning analytics. Journal of Documentation, 75(6), 1333–1355. https://doi.org/10.1108/JD-12-2018-0202

Structured Abstract

Purpose: This study aims to reveal how instructors discuss student data and information privacy in their syllabi.

Design/methodology/approach: The authors collected a mixture of publicly accessible and privately disclosed syllabi from 8,302 library and information science (LIS) courses to extract privacy language. Using privacy concepts from the literature and emergent themes, the authors analyzed the corpus.

Findings: Most syllabi did not mention privacy (98%). Privacy tended to be mentioned in the context of digital tools, course communication, policies, and assignments.

Research limitations/implications (if applicable): The codebook developed during the analysis provides a structure for future research on privacy issues in the higher education context. The transferability of the findings is limited because they address only one field and professional discipline, library and information science, and address syllabi for only online and hybrid courses.

Practical implications (if applicable): The findings suggest a need for professional development for instructors related to student data privacy. The discussion provides recommendations for creating educational experiences that support syllabi development and constructive norming opportunities.

Social implications (if applicable): Instructors may be making assumptions about the degree of privacy literacy among their students or not value student privacy. Each raises significant concerns if privacy is instrumental to intellectual freedom and processes critical to the educational experience.

Originality/value: In an age of educational data mining and analytics, this is one of the first studies to consider if and how instructors are addressing student data privacy in their courses, and the study initiates an important conversation for reflecting on privacy values and practices.

Introduction

The ever-increasing availability of data about people's behavior necessitates continued research and ethic discussion about the collection and use of the data and people's rights to and expectations of privacy. While the concept of information privacy is ambiguous (Solove, 2008), it is best explored in the domain of information science where issues of big data, human computer interaction, and information ethics come together. This study is part of a larger initiative to understand how information and data privacy is conceptualized in the higher education environment. Information science scholars have begun addressing issues associated with student data collection, analysis, and interventions (see Britz & Zimmer 2018; Jones & Salo, 2018; Rubel & Jones, 2016). Additionally, several IMLS-funded projects are exploring the issue from the student and librarian perspective (see Syracuse University, 2017; Trustees of Indiana University, 2018). This study takes an initial step in exploring student privacy from the instructor perspective.

Universities rely on ubiquitous information technology to supports students' educational experiences and run highly bureaucratic institutions. These technologies create flows of data and information that—when captured and organized—make it possible to develop novel insights. Some data practices are required by federal law as part of the 1965 Higher Education Act, but Picciano (2012) comments that over time higher education institutions have developed near-optimal conditions for applying advanced analytic practices beyond simple reporting needs. Where students are concerned, institutions document student life in "digital dossiers" (Solove, 2004) as a prerequisite for admission, and continue to do so as they progress through their program of study. These dossiers are then augmented with the digital trails students leave as they interact with and communicate using institutional information systems, creating rich identifiable content and metadata about their student experiences, social networks, and learning behaviors as they do so (Dawson, 2010).

To support their students, especially online students, and capitalize on the array of data they create, institutions are pursuing Next Generation Digital Learning Environments (NGDLEs). NGDLEs join campus information systems, including the ubiquitous learning management system, to develop infrastructures in support of interoperability, personalization, data analytics, collaboration, and universal and accessible design (Brown, Dehoney, & Millichap, 2015). While state-of-the-art technologies and data practices promise impactful benefits, they also raise significant concerns regarding student privacy.

Aggregating data from campus information systems, as NGDLEs are built to do, opens up access to sensitive types of student data, such as the following: academic, biographic, demographic, financial, system tracking (e.g., logs), communications, and more (see Lederman, 2018; Patel, 2019; Young, 2018). Questions are still open regarding the ethics of collecting these data, as well as analyzing and acting upon them to intervene in

student life. Although information policy and data ethics scholars have taken up these questions, few institutions have; it is even less clear how instructors are discussing these issues with their students, if at all.

With all these things considered, the researchers pursued answers to the following research question: How do distance educators discuss student privacy in their syllabi? Syllabi are central documents in the teaching and learning experience. They convey instructors' values, their disciplinary conventions, emphasize the significance of the course content, and map what students will learn and skills they will gain. Syllabi are also instructional artifacts, detailing to students how to access content and use technologies, among other things. Finally, they are policy documents representing academic rules at different institutional levels (e.g., course, department, school, university), behavioral expectations, and rights associated with state and federal laws. Therefore, it is reasonable to expect that instructors would discuss student privacy in syllabi, especially for distance courses.

1. Literature Review

1.1. Intellectual privacy as a theoretical framework

This article is theoretically framed by the concept of intellectual privacy (Richards, 2015). In education, privacy plays a critical role in processes concerning intellectual contemplation, idea generation, and speech acts expressing one's thoughts and beliefs. There are various facets of privacy that scholars have developed and defended expressing values of privacy, including limiting access to oneself, the ability to control one's information, among others. But where learning is concerned, intellectual privacy provides the protections necessary to introspectively and socially engage in ideation; it provides a "zone of protection" (Richards, 2015, p. 95), specific "places and spaces (real and virtual) in which to read, to think, to explore" (p. 97), which enable individuals to develop "new and possibly heretical ideas…before they are ready" (p. 101) for public reception and scrutiny.

Intellectual privacy maps to concerns regarding student autonomy. Rubel and Jones (2016) explain three reasons for which privacy is intertwined with autonomy. First, privacy enables individuals to "conceive of their goals, projects, and actions as being their own, and not for disclosure to others" (p. 148). Second, and the most common linkage between privacy and autonomy, "others' access to information about one's habits, activities, opinions, feelings, aspirations, and the like can undermine the degree to which one acts or thinks for oneself" (p. 148). Finally, limiting one's access to information "prevents people from seeing aspects of the world and limits their ability to interpret the world" (p. 148). When autonomy is reduced, the ability of individuals to think for themselves, about themselves, and engage in the world around them is limited, and so, too, is their capacity to generate and express ideas.

In different but compatible ways, Richards (2015) and Rubel and Jones (2016) link autonomy—and by extension, privacy—to democratic aims and foundational goals of higher education. For Richards, free speech requires privacy, and through speech democracies (and other forms of government) can be questioned, criticized, and reshaped by the governed. For Rubel and Jones, higher education institutions have a responsibility to promote autonomy (and privacy) because it provides the conditions necessary to prepare students to participate in a liberal democracy by learning skills and values associated with critical thinking, communication, and diversity, among other things (see Bok, 2006; Brighouse, 1998).

Over time, higher education has established roles, developed activities, solidified norms, and used enduring values as references all for the purposes of guiding and governing information flows in ways that protect students' privacy and autonomy interests (Nissenbaum, 2010). However, with learning analytics, there are many open questions regarding the integrity of these strategies. The question in this article is how the syllabus reflects student privacy in an age of learning analytics.

1.2. Learning analytics

The data colleges and universities hold provide pathways forward for improving pedagogy, increasing learning outcomes, and streamlining the administration of bureaucratic institutions. But these opportunities have also emerged because of seismic ontological, epistemological, and axiological shifts in society regarding what to count, how data informs one's worldview, and why data matter above and beyond other ways of knowing (boyd & Crawford, 2012). Taken together, these shifts have brought to the fore a new way to administer and govern higher education: learning analytics (Williamson, 2017).

Capitalizing on growing data stores and using advanced analytical techniques (e.g., dashboards, algorithms, predictive modeling), proponents of learning analytics aim to collect, measure, and analyze visible and once hidden learning behaviors from a variety of academic and non-academic learning environments (Bienkowski, Feng, & Means, 2012; Siemens, 2012). Institutions have adopted learning analytics methods to, inter alia, improve admissions yields (Lloyd, 2014; McGrath, 2014), inform academic advising (Aguilar, Lonn, & Teasley 2014), and help libraries better understand their impact on student success (e.g., retention and graduation) (Jones & Salo, 2018).

Learning analytics technologies aim to describe (what is happening?), diagnose (why did it happen?), predict (what is likely to happen?), and prescribe (what should be done about it?) student learning. Institutions accomplish these tasks using analytics that identify factors that prevent or lead to success, sometimes in classrooms but also throughout a student's life. Where the classroom is concerned, learning analytics often rely on clickstream data, or the so-called timestamped "digital trails" students leave in system logs when they interact with learning management systems and other

educational applications (Ifenthaler & Schumacher, 2016). When clickstream data are combined with student profiles informed by demographic, biographic, socioeconomic, and academic data, institutions can segment their student body and make comparisons among students. Doing so surfaces who is succeeding, when, and the conditions leading to or impeding success.

1.3. Course applications of learning analytics

Student learning is often described in data dashboards within learning analytics systems (Bodily & Verbert, 2017). The dashboards include tables that quantitatively detail actions students take in information systems, and they include visualizations of student behaviors (academic or otherwise) at the individual, cohort, program, or institutional level. Learning analytics dashboards enable institutional actors, like instructors and advisors, to analyze student demographics, actions, and their relation to academic successes and failures in ways different than typical course assessments. One example of learning analytics dashboards is Unizin's student profile report system, which includes aggregate data about a given course's student roster (see Figure 1). The data includes, among other things, students' average age, SAT scores, and academic level (i.e., freshman, sophomore, etc.). Additionally, it provides the course's gender and ethnicity breakdown, in addition to a count of students' GPA scores.

[INSERT FIGURE1.pdf]

Figure 1. The Unizin student profile report system provides aggregate demographic and academic student information (Indiana University, 2018).

It is relevant to note that Unizin deidentifies these data and does not report some data when course enrollments are five students or less. Unizin also developed what it calls its "Snapshot" dashboard, shown in Figure 2, which includes red, yellow, or green graphics to indicate students at academic risk.

[INSERT FIGURE2.pdf]

Figure 2. The Unizin Snapshot dashboard provides green, yellow, and red graphics to quickly identify areas in which a student is successful or unsuccessful (University of Minnesota, 2018). Students names and scores are fictionalized.

It is more often than not the case that instructors have access to learning analytics dashboards, not students. However, the University of Maryland Baltimore County implemented a student-facing dashboard called "Check My Activity." The dashboard shows students a sum of "any hit, click, or access of any tool or content" (Fritz, 2013, p. 2) within the institution's learning management system, and enables students to compare their activity with peers in a course.

Researchers have also written about the use of social network analysis and visualizing networks with sociograms to better understand course networks, especially in online discussion forums. In Figure 3, the sociogram can at a glance show the centrality of the network and the strength of the connections between and among participants.

[INSERT FIGURE3.pdf]

Figure 3. A sample sociogram demonstrating connections in an educational network (Saqr, Fors, Tedre, & Nouri, 2018).

While data tables and visualizations move instructors towards better understanding learner behaviors, they do not predict a student's future state; for this, learning analytics uses predictive modeling to supplement data visualizations. Often, these predictions indicate whether or not a student is at risk of passing a given course (see Figure 4).

[INSERT FIGURE4.pdf]

Figure 4. The second column from the left shows Blackboard's (2018) "probability of passing" predictive score. Students names and scores are fictionalized.

Similar scores are also present in common advising systems, such as EAB's Student Success Collaborative (SSC).[1] But unlike Blackboard, SSC predicts if a student has a chance of success in a given course *before* enrolling. These scores are based on a campus's historical student data regarding academic performance and enrollment trends, among other data points.

A question emerges once analytic systems describe student behaviors and then diagnose and predict student success: What should instructors and other higher education professionals (e.g., advisors) do with the information? Often, learning analytics systems are designed to "nudge" or message students to act. If students are predicted to do poorly in their course or have yet to participate in a weekly online forum, the system can automatically notify students to act, seek help from their instructor, or access learning resources. Systems lacking this nudging capability put the responsibility on instructors to use the information to guide personalized interventions during one-on-one meetings or with respect to adjusting instructional strategies and course content. Some learning systems, such as those provided by Knewton and Pearson, analyze student behaviors and success rates to personalize the content and assessments students receive (Kolowich, 2013).

1.4. Data ethics and privacy problems

[1] EAB was formerly known as the Education Advisory Board.

The ethical issues related to learning analytics track with other data analytics practices, especially those that align with Big Data methods, goals, and interests (Daniel, 2014; Picciano, 2012). Surfacing and acting on sensitive student data raises transparency concerns (Slade & Prinsloo, 2013). It is not clear *who* has access to the growing trove of student data, *what* they are doing with it, and *whether or not* those practices are secure, rigorous, or valid. Since learning analytics increasingly uses black-boxed machine learning-trained algorithms, the transparency issues increase (Mittelstadt, Allo, Taddeo, Wachter, & Floridi, 2016).

Extant arguments suggest that learning analytics and the algorithms that nudge students towards particular courses and programs and away from others create student autonomy issues (Jones, 2017; Rubel & Jones, 2016). The predictive models that score students also raise autonomy concerns, but they also bring to light digital redlining issues when such scores bias instructors in their allocation of time and resources for particular students (Gilliard & Culik, 2016). Some have suggested that even in spite of these unresolved concerns, institutions have a duty of care to act on all possible information (Kay, Korn, & Oppenheim, 2012; Prinsloo & Slade, 2017).

Since many of the ethics issues concern increased access to and uses of identifiable student data and information, researchers have homed in on privacy issues. The literature by and large tends to describe student privacy issues in terms of access, control, and surveillance by answering the following questions:

1) What constraints are there on higher education actors to access student data and use them towards various ends?
2) What rights do students have to control access and use by higher education and third-party actors?
3) Are learning analytics morally acceptable when they enable observation of a student's physical and digital behaviors for the purposes of analysis and intervention?

Where *access* is concerned, researchers are making policy suggestions and frameworks to enable "optimal and ethical harvesting and use of data," and also define who has access rights and under what conditions (Prinsloo & Slade, 2013, p. 240). Access questions and related policies also consider data management and security issues. There exists an ongoing debate about whether or not student datasets should be anonymized or deidentified, especially when some learning analytics goals are to provide personalized resources and services (Baker, 2013; Baker, 2016; Greller & Drachsler, 2012; Peterson, 2012). Stripping data of identifiable characteristics would run counter to these ends, but this assumes more or less deidentification is even possible. Even if institutions were able to deidentify data through extensive data scrubbing and the introduction of data noise, it is increasingly possible to reconstruct or infer an individual's identity with enough datasets (Ohm, 2010).

Access questions tend to focus on an institutional perspective, not that of students, which is what research on *control* aspects of student privacy homes in on. Unlike policy frameworks that can define access restrictions and downstream uses of student data, it is neither clear to what degree students need to be made aware of learning analytics (Willis, Campbell & Pistilli 2013), nor the moral and/or legal obligation institutions have to seek student consent (Slade & Prinsloo, 2013). Assuming consent is practicable—which it often is not (Solove, 2013)—there are related quandaries concerning if consent needs to be active (opt-in), implied (volunteered or inferred), or passive (opt-out). And in cases where students do consent to learning analytics, there are open questions about additional rights students do or do not have to control data about them, such as augmenting, deleting, or selling data (Drachsler & Greller, 2016). Providing students an ability to control identifiable data may curb the utility of learning analytics by limiting the richness of datasets or skewing the representation of the student population (Daries et al., 2014).

Big Data practices elicit fears of government and commercial *surveillance*, and higher education institutions are not immune from such critiques (Slade & Prinsloo, 2013; Prinsloo, 2017). The University of Arizona conducted a three-year study of its freshmen students by tracking their physical movements captured in data when students swiped their student IDs at 700 locations across campus (Blue, 2018). When students were asked about the surveillance aspects of learning analytics, they clearly identified it as an invasion of privacy, expressing that they would be "weirded out" because "everything is being watched" and analyzed (Roberts, Howell, Seaman, & Gibson, 2016, p. 8). As institutions advance their Next Generation Digital Learning Environment infrastructures with advanced data capture and analysis systems and methods, especially as artificial intelligence matures, dataveillance issues will intensify (Selwyn, 2014).

1.5. Student privacy policies

Institutional policy influences data practices and technological design within and beyond institutions, especially with learning analytics vendors (Hoel & Chen, 2016; Prinsloo & Slade, 2013). So, some may argue that instructors should rely on their institution to develop student privacy protections, choosing to let institutional policy documents relay the privacy details to students. But, institutional interests are not necessarily aligned with student interests. In fact, interest among administrators has driven the enthusiasm for learning analytics to-date, not instructors or students (Kregor, Breslin, & Fountain, 2012; Miles, 2015). Instructors cannot trust that their institution will develop fair privacy protections for their students, and thus their overall skepticism towards learning analytics may persist (Corrin, Kennedy, & Mulder, 2013; Howell, Roberts, Seaman, & Gibson, 2017; Polonetsky & Tene, 2014; Rubel & Jones, 2016). Instead of relying on the institution to communicate and dictate student privacy rights, instructors can play a pivotal role.

Student privacy constraints and freedoms depend, in part, on pedagogical choices, instructional designs, and the educational tools instructors adopt (Farah, Vozniuk, Rodríguez-Triana, & Gillet, 2017). Some research suggests that instructors should simply set the default privacy preferences on behalf of their students (Vozniuk et al., 2014). While this is a possibility for educational systems instructors develop themselves, it is not a widespread affordance built into common learning management systems. Waterhouse and Rogers (2004), along with Diaz (2010), make a more feasible suggestion, stating that instructors should develop and embed student privacy policies in their syllabi, as well as link off to existing institutional policies or other relevant privacy resources (such as federal laws, like FERPA). Pointing to extant privacy resources tracks with standard 6.4. of the Quality Matters rubric for higher education (sixth edition), which requires instructors to provide "learners with information on protecting their data and privacy" (Quality Matters, 2018, p.1). The researchers' interest in this paper is centered on how instructors take up these recommendations, if they do, when writing about student privacy in their syllabi.

1.6 The syllabus as evidence of instructor thinking

The syllabus is largely recognized as a critical, central document for a course. In their discourse analysis of syllabi, Afros and Schryer (2009) call it "one of the most recognizable instantiations of academic genres" (p. 225). They claim that, discursively, it conveys the ideology of the course and gives importance to the work the students and instructor will do. In her dissertation examining syllabi in the field of urban education, Campbell (2016) defines syllabi as a "ubiquitous public documents that socialize students into discourse communities" (p. iii). She goes on to say that they "reflect conventions, values, and practices of a discipline" (p. 23).

A characteristic of the syllabus that is particularly relevant to this study is its power to reveal instructor thinking. Parkes and Harris (2002) argue that it is a record of instructor thinking about the course, in that it makes known "the instructor's philosophies about teaching, learning and the content area" (p. 58) as a "profound first impression" (Matjka & Kurke 1994 p. 115). As the initial point of contact in the developing relationship between instructors and students, Denton and Veloso (2018) point out that it is "often the first meaningful piece of information that students receive about a course" (p. 1) and the instructor's ways of thinking. While the syllabus has been studied, especially in the context of library and information science (LIS) education (see Saunders, 2015; VanScoy & Oakleaf, 2008), no current research examines how instructors address student privacy in their syllabi.

2. Research Methods

This study uses document review and thematic analysis to explore how instructors frame the issue of information privacy for students. The course syllabus is a ubiquitous and important evidentiary document of instructor values and thinking and a critical

communication link between instructor and student. While thematically analyzing the syllabi, a codebook was developed to make sense of the privacy issues in the syllabi and to provide a structure for future research.

2.1. Data collection

Syllabi were collected from American Library Association (ALA) accredited, graduate-level library and information science (LIS) programs with at least some distance education component from 2010 to 2017. This time frame covers the period from the emergence of learning analytics to the latest complete year of data. The researchers chose LIS programs as the disciplinary focus because LIS instructors have likely had some exposure to information privacy issues. Even adjunct faculty would likely have some exposure to the issues through professional documents such as the ALA Code of Ethics which specifically mentions privacy. Targeting programs with at least some distance education ensured that instructors would be asking students to use technology that could collect data about them. The researchers were aware that faculty may be sensitive about sharing their syllabi, which represent a significant intellectual property investment. In their IRB-approved recruitment documents and information sheet, the researchers expressed in detail what they would use the syllabi for, how they would secure them, and the strict limits they would place on their access.

When sampling occurred in 2018, there were 61 accredited programs in the United States, Canada, and Puerto Rico (American Library Association, 2018). 52 of 61 programs (~87%) featured some distance education component where student data could be collected. After identifying programs, the researchers began a two-stage process to obtain syllabi. First, they examined the websites of the programs, looking for a syllabi archive; 16 programs listed syllabi on their respective website. For these syllabi, they trained Web Scraper and Folx to download syllabi in HTML and document formats (e.g., PDF, Word).[2] Web scraping resulted in a dataset of 7,008 syllabi. Second, for the remaining 36 programs where syllabi were inaccessible, they solicited syllabi from program directors; five programs supported their request either by providing an archive of syllabi or by directing faculty to individually submit syllabi. This strategy resulted in an additional 1,294 syllabi. The researchers' total dataset included 8,302 syllabi.

2.2. Data analysis procedures

While the dataset was extensive in quantity, the researchers needed to filter it to determine if it met their qualitative interests regarding privacy. To do this, they converted all documents to PDFs, then they ran optical character recognition (OCR) in Adobe Acrobat Pro. With the OCR complete, they keyword searched all 8,000-plus syllabi for "privacy" or "private," resulting in 1,489 hits. Not all of these hits were

[2] Web Scraper is a freely available Chrome extension (http://webscraper.io). Folx is a freely available download manager (https://mac.eltima.com/download-manager.html).

relevant, however. The researchers filtered out results that met at least one of the following conditions:

- Hit was not related to the course;
- Hit was related to course learning material (e.g., modules on privacy, articles with privacy in the title);
- Hit was a duplicate produced by Adobe due to nearby instances of "privacy" or "private" in a line of text;
- Hit was for a course outside the 2010-2017 year range;
- Hit was for a non-graduate course;
- Hit was for a researcher's own course.

These efforts scaled down the relevant number of hits to 188 within 174 syllabi (including duplicate language across syllabi), representing 14 programs.

Each researcher independently applied deductive codes based on their understanding of the literature to a sample of the 188 hits and developed thematic codes at the same time. Following, the researchers discussed emergent codes, reconciled similar codes, and removed both deductive and inductive codes that were no longer relevant. Researchers further developed the codes by arranging them into "families" of conceptually alike codes. To enhance rigor, the researchers took extensive notes about analytical and methodological decisions. Finally, the researchers individually coded all 188 hits using the finalized codebook before coming together once again to ensure that codes were applied accurately (see the codebook in Appendix A). The development of the codebook was rigorous and the corpus studied was significant, albeit limited to one scholarly field and associated discipline. The researchers have confidence that the findings discussed below are likely to transfer to other syllabi that meet the same sampling requirements.

3. Findings

3.1. Prominent code categories

Only 2% of the syllabi examined included language relating to privacy. Of this 2%, the top code categories suggest that instructors most prominently include privacy language when describing tools and tool usage, addressing communication norms and expectations, relaying institutional policies, and describing assignments and assessment practices when discussing privacy in their syllabi.

Nearly 36% of syllabi that included some mention of privacy included substantive privacy language when discussing tools. For example, institutional learning management systems (e.g., Blackboard, Canvas), Google tools (e.g., Drive, Sheets), social media (e.g., Twitter, Facebook), and content management systems (e.g., WordPress) were

prominent foils against which to discuss privacy. When describing tool usage, instructors would discuss ways in which students should have a limited expectation of privacy; this was often the case with third-party tools like Google. But when discussing institutional tools, like e-mail and learning management systems, instructors would sometimes suggest that students could expect more privacy.

Another 35% of syllabi that mentioned privacy included privacy language when addressing communications, such as peer-to-peer and peer-to-instructor. Here, syllabi set expectations for holding private communications, provided information on the limitations of holding private communications, or often times instructed students on how to hold private communications. 65% of the data within this theme situated communication practices against specific tools, such as institutional e-mail systems, learning management systems and their specific affordances (e.g., discussion boards, group sites), and third-party applications.

About 32% of syllabi that mentioned privacy addressed privacy in relation to institutional policies. Drilling down into these data, the researchers found a mixture of ways that instructors used privacy language. 42% of the data in this theme linked to institutional privacy policies, while only 35% included unique privacy policies. Other privacy policy language was subsumed under broader academic freedom policies, representing 22% of the theme's data.

A little more than 28% of syllabi that mentioned privacy discussed it in relation to assignment descriptions and assessment activities. And it was often the case that this category of data dovetailed with discussions of tools and communications. This suggests that many of the assignments included specific tools, and instructors wanted their students to be aware of how usage of these tools may impact their privacy. In the following sub-sections, the researchers detail more of the qualitative aspects of these findings.

3.2. Instructions and alternatives

When discussing tools used in their courses, instructors spent effort in their syllabi to instruct their students on how to protect their privacy. Often, these instructions concerned how students could change setting defaults in order to achieve more privacy. Instructors referenced tools like YouTube in discussing how to set online content to be private or unlisted, so as to limit disclosure of information to particular audiences, like their peers and instructor. Another instructor detailed information on how to make blog posts visible to particular users. Notably, one instructor provided detailed, step-by-step instructions for different browsers to help students delete their web history and cache.

Some instructors commented on the inherent privacy problems associated with disclosing information online. For example, an instructor stated, "First and foremost in electronic communication: it is not very private and secure. Don't write what you

wouldn't feel comfortable having on the front page of the New York Times. Remember that your communication may be archived and searchable for years later." The instructor continued her warning with examples of archived online communications by providing articles arguing that privacy was "dead" and news stories cautioning job seekers about how their online presence could be used against them on the job market. Another instructor put the duty to protect one's privacy solely on his students' shoulders, stating:

> When interacting online, please use your best judgment. You are solely responsible for the privacy of your information, the safety and quality of your experience, and the legality and appropriateness of all your actions online. Make yourself aware of the privacy policy of the services you are using, the user rules and guidelines, as well as any safeguards you should take online.

Other instructors contrasted institution-provided tools against third-party tools, detailing how the former are governed by privacy policies unique from those of the latter. About this, an instructor wrote:

> When using online resources offered by organizations not affiliated with [the university], such as Google or YouTube, please note that the terms and conditions of these companies and not [the university's] Terms and Conditions apply. These third parties may offer different degrees of privacy protection and access rights to online content. You should be well aware of this when posting content to sites not managed by [the university].

Instructors also provided information on how their students can respect the privacy of their peers within the course and others whose privacy could be affected by course artifacts. This information highlighted the importance of peer-to-peer privacy and sometimes addressed the potential harms of disclosing private information. One instructor directed students to ask permission from peers before revealing identifiable information, including e-mail addresses. Another instructor directed students to not include information in a portfolio assignment when:

> […] such use would violate someone's right of privacy (or right of publicity) by revealing personally identifiable information such as a person's name, likeness (image) or contact information. Care should always be given in upholding privacy rights […] personal identification can be inferred […] even absent name and contact information. In most privacy cases, redacting the personally identifiable information is sufficient.

Many instructors reminded their students about the visibility settings of different tools, especially blogs and discussion boards. They would make comments like "any message posted to this space can be read by ALL of your classmates," and they discussed how more privacy can be achieved by sending communications and coursework directly to

the instructor via e-mail instead of posting to course community platforms, like a learning management system.

To resolve some privacy problems, instructors provided students alternatives by which they could participate in courses while protecting their identities and personally identifiable information. In these data, instructors clearly indicated that students should, first, communicate their privacy preferences with their instructor, and, second, choose among a set of privacy-enhancing options. Instructors were clear to state that student preferences needed to be expressed *before* participating in activities or engaging with tools that could compromise their privacy, in so doing reflecting an awareness that disclosed information may not be able to be retracted. Alternatives included giving students the option to publish coursework and communicate with peers using pseudonym, which some instructors directed students to do when using third-party tools. In cases where students used pseudonyms, they were required to unmask themselves to their instructor for assessment purposes.

3.3. Information disclosure: Anonymity and confidentiality

Instructors referenced anonymity and confidentiality over 20 times. These data used anonymity in reference to students' identities but skewed towards using confidentiality with respect to student information, especially student records. For instance, one instructor used Slack, the online team collaboration platform, as an alternative to her institution's learning management system. She stated that Slack ensured anonymity with regard to course population and its activities. Another instructor made a similar claim about social media platforms:

> I might ask you to consider using any number of social media tools. These are optional, and I can work with you if you are either uncomfortable using them or simply do not want to. I'm using them to make communication more convenient for YOU! Some of the tools (Twitter) allow anonymity--use that if you want.

Similar statements were made about using institutional tools, such as posting to learning management system discussion boards, when privacy-protecting affordances existed to allow anonymous participation, such as: "you can also choose to have your notes and questions visible to the entire class but anonymous to other students (I will still be able to see who left the note)."

Of the 15 instances of language related to confidentiality, five were in relation to student records and the other 10 were associated with the communication of private information. Several syllabi from one institution stated that "under the Family Educational Rights and Privacy Act (FERPA), [student] records are confidential and protected," while another syllabus provided a link to an institutional webpage on the confidentiality of student records. When discussing communications, several instructors positioned privacy as something different from confidentiality, stating that if

communications were not "private or confidential," then they should be published at the course website. Another instructor explicitly defined confidentiality as the non-disclosure of information of others as a means by which to protect privacy.

3.4. Federal and institutional privacy rights

As alluded to in the previous sub-section, some syllabi explicitly addressed federal student privacy law, namely FERPA. Others referenced institutional student privacy policies. In both cases, instructors expressed various privacy rights and limitations.

When instructors wrote about privacy rights and responsibilities, they explicitly addressed institutional policies and/or FERPA. Some instructors would also link to relevant institutional policies or the institution's webpage discussing FERPA to encourage students to "learn more." It is notable that in these cases, there was significant repetition across syllabi, which the researchers argue represents standardized privacy language.[3] Specifically, these syllabi noted particular rights to privacy with some limitations, including:

- [Students have a] FERPA right to keep [their] educational record, including enrollment in any specific class, private"
- "[Student] records are confidential and protected"
- "Under most circumstances [student] records will not be released without [the student's] written and signed consent"
- "Some directory information may be released to third parties without [the student's] prior consent unless a written request to restrict [disclosure] is on file"
- "The redistribution of audio or video recordings of statements or comments from the course to individuals who are not students in the course is prohibited without the express permission of the faculty member and of any students who are recorded"

In a few instances specifically related to language about institutional policies, instructors noted that disclosing private information could violate specific academic codes and result in disciplinary action, but they were more ambiguous about repercussions when discussing privacy and copyright laws.

Regarding limits on privacy rights, some instructors specifically stated that any privacy rights guaranteed by FERPA and addressed in institutional policy no longer apply when students use third-party tools. As one instructor wrote to her students, "this has significant implications for FERPA regulations about your personal privacy and the privacy of your student records." Another instructor claimed that "because of [FERPA], you must use your secure [university] accounts for email communication." When FERPA and their institution could no longer provide comprehensive privacy protections, some instructors made their students aware of their duty to shore up these gaps. To do so,

[3] With the data the researchers have, they do not know if such language originated at the program, department, school, or university level.

instructors wrote in their syllabi that it was their responsibility to read the privacy policies of particular tools in order to "use good judgment" with respect to disclosing their personal information and that of their peers.

3.5. The role of privacy in learning

25 syllabi originating from two institutions expressed the "inviolate right of privacy" and its role in learning. As with some language related to FERPA, there was notable redundancy, signaling that these data represent standardized syllabi language. Both institutions similarly stated that students' "views, beliefs, and political associations" or "information about the ideas they express, their families, life styles and their political and social affiliations" must be handled carefully and respectfully.

Treating such information with care, the instructors wrote, was necessary because "learning often requires uncomfortable growth" since students "often wrestle with critical issues" that require the flexibility and opportunity to change positions, views, and values. As stated in the syllabi, "privacy is an important and necessary part of the educational process" because it supports "an academic environment of rigorous discussion and open expression of personal thoughts and feelings." Should students' privacy not be protected, harms could accrue.

Disclosure or mistreatment of private student information may subject students to "ridicule, harassment, or reprisal from those who do not agree with the views, beliefs, or political associations expressed in the context of the classroom." A set of syllabi stated that the purpose of the privacy notice was to "make sure that students are not embarrassed for things they may have said or done while in the process of intellectual growth." In cases where students would be unaware of the consequences of disclosing private information, an institution's syllabi encouraged its students to "ask the instructor for guidance."

4. Discussion

4.1. Reflections on missing privacy information

The most striking finding concerns the scarcity of privacy in the studied corpus. Only two percent of the studied syllabi (174 of 8,302 syllabi) had any substantive language regarding student privacy. The absence of data leads to more questions than answers, and pursuing this line of questioning does not promote the project's transferability; yet, speculating as to why privacy is missing in so many syllabi is still a useful endeavor.

Given privacy's absence in syllabi, one notable explanation may be that student privacy is not valued by most instructors. If syllabi are expressions of instructional values, then it follows that *not* writing about privacy means that instructors find it to be neither instrumental to learning nor intrinsically valuable. Thus, instructors believe it is simply

not necessary to discuss privacy in their syllabi. While this may be the case for some instructors, the researchers find this explanation suspect given values embraced by the library and information science (LIS) profession, which LIS faculty teach and generally promote.

The American Library Association (ALA), the International Federation of Library Associations and Institutions (IFLA), the Association of Research Libraries (ARL), and many others worldwide express in, inter alia, their focus areas, mission statements, and code of ethics that privacy is valued (Klinefelter, 2010; Koehler, 2006; Shachaf, 2005). These documents argue that privacy is part and parcel for intellectual freedom since it protects individuals from unwarranted influence. As such, the documents are often included as assigned reading materials in LIS courses to support discussions about professional ethics and informational privacy. Since privacy is emphasized so heavily in LIS education and professionalization strategies, its omission from syllabi is striking. But perhaps another reason for the omission is that syllabi are simply bloated.

There may be little motivation to include privacy policies and instructions, among other things, given the fact that syllabi continue to balloon in size, regardless of instructor effort. Institutions increasingly require their faculty to include a variety of policy language (e.g., academic integrity, attendance, behavior, etc.), leading to proliferating page counts. Some of these efforts are motivated by an instructional design philosophy arguing that more information tends to guide students towards success, while other motivations stem from the fact that syllabi are treated as contractually binding, pseudo-legal documents that need to account for possible liabilities (Alberts, Hazen, & Theobald, 2010; Wasley, 2008). If there is no requirement to include privacy language, some faculty might prefer to exclude it to trim down syllabi length.

The above explanations for missing privacy language are speculative, even though some are motivated by the researchers' understanding of the literature and expert knowledge about the profession (and teaching for the profession). Answers to these questions require data that the research described herein could not provide, and future work in this area should seek these answers from faculty (see section 4.4. for more).

4.2. The importance of accuracy when talking about privacy

The Family Educational Rights and Privacy Act (FERPA) and institutional policies describe student privacy rights and responsibilities. As such, these are crucial policy documents, and discussing them accurately and clearly is important. The findings indicate, however, that much of the language used in this area is ambiguous and requires privacy literacies that instructors cannot assume their students possess; some instructors even need retraining on FERPA themselves. Moreover, simply linking to such policies may not motivate students to review them, neither will quoting policy language change their privacy practices (see Gullifer & Tyson, 2010).

Instructors cannot take for granted that students understand key terms, like what an educational record is or how a third-party tool is defined. Critical analysis of FERPA has shown that against the backdrop of learning analytics and educational data mining, it is increasingly difficult to pin down how to define an educational record and what data and information such records enclose (Polonetsky & Tene, 2015; Rubel & Jones, 2016). When instructors do use FERPA to motivate student privacy behavior, they need to be precise. For instance, data indicated that students were told they were required to use institutional e-mail systems *because of* FERPA; this is incorrect. FERPA does not require the use of any particular tool, but students do have enhanced privacy protections when using institutional tools. This is so because universities vet contracts and memoranda of understanding with educational technology providers who gain access to institutionally managed identifiable information, and those agreements typically bind providers as "school officials" who must abide by FERPA (Polonetsky & Jerome, 2014).

Students interact with a medley of educational technologies, especially when pursuing their degree from a distance. It is challenging, if not nigh impossible for students to determine which tools are institution-sanctioned and which third-party tools are just preferred for use by the instructor. Even in cases where institutions have vetted particular tools, it does not necessarily follow that these systems do not have access to sensitive student data, especially private communications and profile data. Additionally, students should not be led to believe that the systems will not use data to serve their own interests, such as for data sales (Canvas, 2015; Hill, 2016), advertising (Kelly, Graham, & Fitzgerald, 2018), or product testing purposes (Strauss, 2018).

Stating that student data and information will be kept confidential or anonymous, as instructors did, and that records are protected leads raises other issues. First, instructors sometimes used "confidentiality" and "anonymity" interchangeably, which misleads students. While it may be the case that instructors will hold student data and information in confidence, if entered into an educational technology system, that same data and information may be subsumed into an institutional data warehouse for analysis and downstream disclosure to actors within and outside the student's institution (see Young, 2018). And even in cases where data is anonymous, such as when students use a pseudonym on Twitter, research has shown that combining datasets decreases the integrity of anonymous data (Ohm, 2010).

4.3. Embedding privacy values into syllabi and creating new norms

Not a single syllabus represented all codes, so it is fair to say that privacy is valued in particular ways depending on a combination of practice, policy, knowledge, and situation—or more broadly the context in which privacy language is situated. This sociotechnical complexity makes it challenging to talk about privacy and consider what to include in syllabi. But, the complexity of the situation cannot be used as an excuse for not addressing increasing student privacy issues. Whether instructors approve or not of the collection of student data or intend to make use of it, the reality is that student data

are being collected. Instructors, therefore have an obligation to be informed about the issues, relevant policies, and expected practices, as well as the ethical implications.

Current and future instructors need opportunities to learn about the ethical issues surrounding student data privacy, as well as opportunities to discuss the issues and make informed choices for their courses. Instructors in all roles—teaching assistants, adjunct faculty, librarians, and tenure-track/tenured/non-tenure track faculty—need professional development on information privacy in an age of learning analytics. University teaching and learning offices could take up a leadership role in providing such education, but so could libraries, whose understanding of the value of privacy in intellectual environments would add insight to these educational conversations. Two positive outcomes could arise from professional development.

First, instructors would be able to learn, express, and justify the privacy decisions they make when developing courses and syllabi. As Campbell (2016) and Parkes and Harris (2006) have argued, the syllabus is partly an expression of values. So, enabling reflection on one's values and providing time to articulate these values to peers is a worthwhile venture. If instructors work with and learn from instructional designers, librarians, technologists, and administrators, they will gain a thorough understanding of flows of student data and information, the value thereof and related risks, and how to protect students. These conversations may also help instructors better understand what institutional, state/provincial, and federal laws govern student privacy, which may improve their ability to develop syllabi policy, curate privacy resources (e.g., technology privacy policies), and provide more accurate language about key terms, privacy rights and, responsibilities to protect one's privacy.

Second, articulating and discussing student privacy will inevitably reveal competing priorities and differences in value propositions. These discussions, however contentious they may become, should be seen in a positive light as they seed opportunities to reflect on established norms and provide circumstances necessary for developing new norms. The community of instructors may norm amongst themselves within a department or a professional community, such as the Association of Library and Information Science Education. Similarly, faculty may norm with their administrative colleagues who have different justifications for aggregating and analyzing student data. At the University of California (2017) and University of Hawaii (2018), these efforts have helped establish resolutions to protect learner data and privacy. Norming may also happen at the level of the learning community. Instructors who invite students into the data privacy conversation demonstrate the value of students' privacy and can improve students' privacy literacy. For this to occur, instructors must be willing to alter policies and procedures, but in exchange, they will empower students to consider their rights and responsibilities and advocate for themselves.

4.4. An Emerging Research Agenda

While the study's findings reveal how syllabi discuss student privacy and help seed important conversations about student privacy, the study has limitations—limitations that lead to a growing research agenda for the authors and others to pursue. Syllabi do not explain the reasons why privacy language is or is not included; they cannot speak for themselves. Since the data are inherently limited and the article's methodology cannot uncover underlying reasons, more research is necessary with instructors to determine why certain privacy decisions are or are not made and why. To address these issues, the authors propose the following lines of inquiry, many of which they have outlined in a full grant proposal currently under review.

More research is needed with other disciplines to see if thematic findings differ in substantial ways from LIS instructors, as well as with instructors who do not teach online. Surveys can investigate how instructors understand student privacy and make related instructional choices, in addition to their understanding of how their institutions use and protect student data. Instructor demographics (e.g., full-time, adjunct, course load) and institutional demographics (e.g., community college, research-intensive institutions) may be statistically explanatory. Interviews with survey participants would allow researchers to probe into issues of values, ethics, and conditions that promote or inhibit student privacy in non-syllabi instructional artifacts (e.g., online course sites) and activities (e.g., lectures, groupwork). To different degrees, surveys and interviews could also investigate an instructor's student privacy literacy and the privacy resources they reference.

This study is conceived as a critical first step in exploring information privacy from the instructor perspective. Syllabi are important to study as instantiations of instructional student privacy choices, practices, and communications. The make visible how instructors attempt to address (or not) student privacy in their courses. Even without data that will come from the future research agenda, the aforementioned findings provide useful insights for instructors as they consider if and how to address student privacy in their syllabi. They also may inform governing bodies, such as departmental committees and institutional working groups, when developing student privacy policies.

5. Conclusion

Examining the syllabus—a critical document that serves as a tool for communication, learning, and rule-setting, as well as an expression of values—reveals a breadth of student data privacy issues and practices in LIS courses. It also reveals challenges associated with this issue, including accurately explaining privacy concepts and ensuring that students have adequate privacy literacy. Facilitating reflection and discussion among instructors about student data privacy in the syllabus may help to alleviate some

of these challenges and strengthen the syllabus as a useful document in empowering students to value and protect their own data privacy.

Higher education institutions are increasing their interest in and capacity for mining and analyzing student life with learning analytics. And while institutions have a responsibility to consider student privacy in policy and technological design, instructors bear a responsibility as well. Whether or not instructors gather, analyze, and act upon student data, someone or something is. Instructors need to take responsibility for the ways their instructional designs affect student privacy and how they discuss privacy with their students, in syllabi or otherwise.

References

Afros, E., & Schryer, C. F. (2009), "The genre of syllabus in higher education", *Journal of English for Academic Purposes*, Vol. 8 No. 3, pp. 224–233, doi: 10.1016/j.jeap.2009.01.004.

Aguilar, S., Lonn, S. & Teasley, S.D. (2014), "Perceptions and use of an early warning system during a higher education transition program", in *Proceedings of the fourth international conference on learning analytics and knowledge*, ACM, pp. 113–117, doi: 10.1145/2567574.2567625.

Alberts, H. C., Hazen, H.D., & Theobald, R. B. (2010), "Classroom incivilities: The challenge of interactions between college students and instructors in the US", *Journal of Geography in Higher Education,* Vol. 34 No. 3, pp. 439–462, doi: 10.1080/03098260903502679.

American Library Association (2018, June 18), "Directory of institutions offering ALA-accredited master's programs in library and information studies", available at: http://www.ala.org/CFApps/lisdir/directory_pdf.cfm.

Baker, R. S. J. d. (2013), "Learning, schooling, and data analytics", in Murphy, M., Redding, S., & Twyman, J. (Eds.), *Handbook on innovations in learning for states, districts, and schools,* Temple University, Center on Innovations in Learning, Philadelphia, PA, pp. 179–190.

Baker, R. (2016), "Using learning analytics in personalized learning", in Murphy, M., Redding, S., & Twyman, J. (Eds.), *Handbook on personalized learning for states, districts, and schools,* Temple University, Center on Innovations in Learning, Philadelphia, PA, pp. 165–174.

Bienkowski, M., Feng, M., & Means, B. (2012), *Enhancing teaching and learning through educational data mining and learning analytics: An issue brief*, U.S. Department

of Education, available at: http://tech.ed.gov/wp-content/uploads/2014/03/edm-la- brief.pdf.

Blackboard. (2018), "Blackboard Predict help for instructors," available at: https://help.blackboard.com/Predict/Instructor.

Blue, A. (2018, March 7), "Researcher looks at 'digital traces' to help students", University of Arizona News, available at: https://uanews.arizona.edu/story/researcher-looks-digital-traces-help-students.

Bodily, R., & Verbert, K. (2017), "Trends and issues in student-facing learning analytics reporting systems research", in *Proceedings of the Seventh International Conference on Learning Analytics and Knowledge,* Canada*,* pp. 309–318, doi: 10.1145/3027385.3027403.

Bok, D. C. (2006), *Our underachieving colleges: A candid look at how much students learn and why they should be learning mor*e, Princeton University Press, Princeton, NJ.

boyd, d., & Crawford, K. (2012), "Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon", *Information, Communication & Society,* Vol. 15 No. 5, pp. 662–679, doi: 10.1080/1369118X.2012.678878.

Brighouse, H. (1998), "Civic education and liberal legitimacy", *Ethics*, Vol. 108 No. 4, pp. 719–745, doi: 10.1086/233849

Britz, J., & Zimmer, M. (2014), "The digital futures of education: An introduction", *International Review of Information Ethics*, Vol. 21 No. 7/2014, p. 2, available at: http://www.i-r-i-e.net/issue21.htm

Brown, M., Dehoney, J., & Millichap, N. (2015), *The next generation digital learning environment: A report on research*, EDUCAUSE, available at: https://library.educause.edu/~/media/files/library/2015/4/eli3035-pdf.pdf

Campbell, J. M. (2016), "Theme and variations: A content analysis of syllabi in introduction to urban education courses" (Doctoral dissertation), available at: ProQuest Dissertations (Dissertation number 10111285).

Canvas. (2015, June 18), "Instructure launches Canvas Data, a new data optimization service for academic institutions" [Press release], available at: https://www.canvaslms.com/news/press-releases/instructure-launches-canvas-data.

Corrin, L., Kennedy, G., & Mulder, R. (2013), "Enhancing learning analytics by understanding the needs of teachers", in *Proceedings of Electric Dreams: The 30th Ascilite Conference,* Australia, pp. 201–205, available at: http://ascilite.org/conferences/sydney13/program/papers/Corrin.pdf

Daniel, B. (2014), "Big Data and analytics in higher education: Opportunities and challenges", *British Journal of Educational Technology,* Vol. 46 No. 5, pp. 904–920, doi: 10.1111/bjet.12230.

Daries, J. P., Reich, J., Waldo, J., Young, E. M., Whittinghill, J., Ho, A.D., Seaton, D. T., & Chuang, I. (2014), "Privacy, anonymity, and big data in the social sciences", *ACM Queue,* Vol. 12 No. 7, pp. 1–12, available at: https://queue.acm.org/detail.cfm?id=2661641.

Dawson, S. (2010), "'Seeing' the learning community: An exploration of the development of a resource for monitoring online student networking", *British Journal of Educational Technology,* Vol. 41 No. 5, pp. 736–752, doi: 10.1111/j.1467-8535.2009.00970.x.

Denton, A. W., & Veloso, J. (2018), "Changes in syllabus tone affect warmth (but not competence) ratings of both male and female instructors", *Social Psychology of Education,* Vol. 21 No. 1, pp. 173–187, doi: 10.1007/s11218-017-9409-7.

Diaz, V. (2010), "Web 2.0 and emerging technologies in online learning", in *New Directions for Community Colleges,* New Jersey: Wiley Periodicals, pp. 57–66, doi: 10.1002/cc.405.

Drachsler, H., & Greller, W. (2016), "Privacy and analytics—it's a DELICATE issue: A checklist for trusted learning analytics", in *Proceedings of the Sixth International Conference on Learning Analytics and Knowledge,* UK, pp. 89–98, doi: 10.1145/2883851.2883893.

Farah, J. C., Vozniuk, A., Rodríguez-Triana, M. J., & Gillet, D. (2017), "A teacher survey on educational data management practices: Tracking and storage of activity traces," Paper presented at the 10th Workshop on Ethics & Privacy in Learning Analytics @ EC-TEL 2017, Tallinn, Estonia, available at: https://infoscience.epfl.ch/record/231023/files/2017___EC_TEL___Ethics___Privacy_in_Learning_Analytics_Workshop.pdf.

Fritz, J. (2013), *Using analytics at UMBC: Encouraging student responsibility and identifying effective course designs*, EDUCAUSE, available at: https://net.educause.edu/ir/library/pdf/ERB1304.pdf.

Gilliard, C., & Culik, H. (2016, May 24), "Digital redlining, access, and privacy", *Common Sense Education*, available at: https://www.commonsense.org/education/privacy/blog/digital-redlining-access-privacy.

Greller, W., & Drachsler, H. (2012), "Translating learning into numbers: A generic framework for learning analytics," *Journal of Educational Technology & Society,* Vol. 15 No. 3, pp. 42–57, available at: http://www.ifets.info/download_pdf.php?j_id=56&a_id=1256.

Gullifer, J., & Tyson, G. A. (2010), "Exploring university students' perceptions of plagiarism: A focus group study", *Studies in Higher Education,* Vol. 35 No. 4, pp. 463–481, doi: 10.1080/03075070903096508.

Hill, P. (2016, November 10), "Popular discussion platform Piazza getting pushback for selling student data", *eLiterate*, available at: https://mfeldstein.com/popular-discussion-platform-piazza-getting-pushback-selling-student-data/.

Hoel, T., & Chen, W. (2016), "Privacy-driven design of learning analytics applications – Exploring the design space of solutions for data sharing and interoperability", *Journal of Learning Analytics,* Vol. 3 No. 1*,* doi: 10.18608/jla.2016.31.9.

Howell, J. A., Roberts, L. D., & Seaman, K. (2017), "Are we on our way to becoming a 'Helicopter University'? Academics' views on learning analytics", *Technology, Knowledge and Learning,* Vol. 23 No. 1, pp. 1–20, doi: 10.1007/s10758-017-9329-9.

Ifenthaler, D., & Schumacher, C. (2016), "Student perceptions of privacy principles for learning analytics", *Educational Technology Research and Development,* Vol. 64 No. 5, pp. 923–938, doi: 10.1007/s11423-016-9477-y.

Indiana University. (2018), "Student profile report info-share", available at: https://iu.box.com/s/0hi0cplwkdp51zum99fy8sh10cvqr1uu.

Jones, K. M. L. (2017), "Learning analytics and its paternalistic influences", in Zaphiris, P. & Ioannou, A. (Eds.), *Lecture Notes in Computer Science, Learning and Collaboration Technologies: Technology in Education (LCT 2017, HCI International 2017)*, Springer, pp. 281–292, doi: 10.1007/978-3-319-58515-4_22.

Jones, K. M. L., & Salo, D. (2018), "Learning analytics and the academic library: Professional ethics commitments at a crossroads", *College & Research Libraries,* Vol. 79 No. 3, pp. 304–323, doi: 10.5860/crl.79.3.304.

Kay, D., Korn, N., & Oppenheim, C. (2012), "Legal, risk, and ethical aspects of analytics in higher education, Vol. 1 No. 6.", JISC Centre for Educational Technology & Interoperability Standards, available at: http://publications.cetis.org.uk/wp-content/uploads/2012/11/Legal-Risk-and-Ethical-Aspects-of-Analytics-in-Higher-Education-Vol1-No6.pdf.

Kelly, G., Graham, J., & Fitzgerald, B. (2018), *2018 state of edtech privacy report* (The Common Sense Privacy Evaluation Initiative), Common Sense, San Francisco, CA, available at: https://www.commonsense.org/education/sites/default/files/tlr-blog/cs-state-of-edtech-privacy-report.pdf.

Klinefelter, A. (2010), "Library standards for privacy: A model for the digital world", *North Carolina Journal of Law & Technology,* Vol. 11 No. 3, pp. 553–564, available at: https://heinonline.org/HOL/P?h=hein.journals/ncjl11&i=560.

Koehler, W. (2006), "National library associations as reflected in their codes of ethics: Four codes examined", *Library Management,* Vol. 27 No. 1/2, pp. 24–35, doi: 10.1108/01435120610647974.

Kolowich, S. (2013, January 25), "The new intelligence", *Insider Higher Ed*, available at: http://www.insidehighered.com/news/2013/01/25/arizona-st-and-knewtons-grand- experiment-adaptive-learning.

Kregor, G., Breslin, M., & Fountain, W. (2012), "Experience and beliefs of technology users at an Australian university: Keys to maximising e-learning potential", *Australasian Journal of Educational Technology,* Vol. 28, pp. 1382–1404, doi: 10.14742/ajet.777.

Lederman, D. (2018, September 5), "Unizin chooses new leaders, launches data Platform", *Inside Higher Ed*, Available at: https://www.insidehighered.com/digital-learning/insights/2018/09/05/unizin-chooses-new-leaders-launches-data-platform

Lloyd, T. (2014, January 14), "How college applications change in the era of big data", *Marketplace*, available at: https://www.marketplace.org/2014/01/14/education/how-college-applications-change-era-big-data.

McGrath, M. (2014, July 30), "The invisible force behind college admissions", *Forbes*, available at: https://www.forbes.com/sites/maggiemcgrath/2014/07/30/the-invisible-force-behind-college-admissions/.

Miles, C. (2015), "Australian university teachers' engagement with learning analytics: Still early days", in *Proceedings of EdMedia: World Conference on Educational*

Media and Technology, Canada, p. 108, available at: https://www.learntechlib.org/p/151474/.

Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016), "The ethics of algorithms: Mapping the debate", *Big Data & Society,* Vol. 3 No. 2, pp. 1–21, doi: 10.1177/2053951716679679.

Ohm, P. (2010), "Broken promises of privacy: Responding to the surprising failure of anonymization", *UCLA Law Review*, Vol. 57, pp. 1701–1777, available at: https://www.uclalawreview.org/pdf/57-6-3.pdf.

Parkes, J. & Harris, M. B. (2002), "The purpose of a syllabus", *College Teaching,* Vol. 50 No. 2, pp. 55–61, doi: 10.1080/87567550209595875.

Patel, V. (2019, April 9), "Are students socially connected? Check their dining-hall-swipe data", *The Chronicle of Higher Education*, available at: https://www.chronicle.com/article/Are-Students-Socially/246077

Picciano, A. (2012), "The evolution of big data and learning analytics in American higher education", *Journal of Asynchronous Learning Networks,* Vol. 16 No. 3, pp. 9–20.

Polonetsky, J., & Jerome, J. (2014), "Student data: Trust, transparency, and the role of consent" (Future of Privacy Forum Report), available at: https://fpf.org/wp-content/uploads/FPF_Education_Consent_StudentData_Oct2014.pdf.

Polonetsky, J., & Tene, O. (2014), "The ethics of student privacy: Building trust for ed tech", *International Review of Information Ethics,* Vol. 21, pp. 25–34, available at: http://www.i-r-i-e.net/inhalt/021/IRIE-021-Polonetsky-Tene.pdf.

Polonetsky, J., Tene, O. (2015), "Who is reading whom now: Privacy in education from books to moocs", *Vanderbilt Journal of Entertainment and Technology Law,* Vol. 17 No. 4, pp. 927–990, available at: https://heinonline.org/HOL/P?h=hein.journals/vanep17&i=961.

Picciano, P. (2017), "Fleeing from Frankenstein's monster and meeting Kafka on the way: Algorithmic decision-making in higher education", *E-Learning and Digital Media,* Vol. 14 No. 3, pp. 138–163, doi: 10.1177/2042753017731355.

Prinsloo, P. & Slade, S. (2013), "An evaluation of policy frameworks for addressing ethical considerations in learning analytics", in *Proceedings of the Third International Conference on Learning Analytics and Knowledge,* Belgium, pp. 240–244, doi: 10.1145/2460296.2460344.

Prinsloo, P., & Slade, S. (2017), "An elephant in the learning analytics room – the obligation to act", in *Proceedings of the Seventh International Conference on Learning Analytics and Knowledge,* Canada, pp. 46–55, doi: 10.1145/3027385.3027406.

Quality Matters. (2018), "Specific review standards from the QM higher education rubric, sixth edition", available at: https://www.qualitymatters.org/sites/default/files/PDFs/StandardsfromtheQMHigherEducationRubric.pdf.

Richards, N. (2015), *Intellectual privacy: Rethinking civil liberties in the digital age*, Oxford University Press, Oxford, UK.

Roberts, L. D., Howell, J. A., Seaman, K., & Gibson, D. C. (2016), "Student attitudes toward learning analytics: 'The Fitbit version of the learning world'", *Frontiers in Psychology,* Vol. 7 No. 1959, pp. 1–11, doi: 10.3389/fpsyg.2016.01959.

Rubel, A. & Jones, K. M. L. (2016), "Student privacy in learning analytics: An information ethics perspective", *The Information Society,* Vol. 32 No. 2, pp. 143–159, doi: 10.1080/01972243.2016.1130502.

Saqr, M., Fors, U., Tedre, M., & Nouri, J. (2018), "How social network analysis can be used to monitor online collaborative learning and guide an informed intervention", *PLoS ONE,* Vol. 13 No. 3, pp. 1–22, doi: 10.1371/journal.pone.0194777.

Saunders, L. (2015), "Education for instruction: A review of LIS instruction syllabi", *Reference Librarian,* Vol. 56 No. 1, pp. 1–21, doi: 10.1080/02763877.2014.969392.

Selwyn, N. (2014), *Digital technology and the contemporary university: Degrees of digitization*, Routledge, London, UK.

Shachaf, P. (2005), "A global perspective on library association codes of ethics", *Library & Information Science Research,* Vol. 27 No. 4, pp. 513–533, doi: 10.1016/j.lisr.2005.08.008.

Siemens, G. (2012), "Learning analytics: Envisioning a research discipline and a domain of practice", in *Proceedings of the Second International Conference on Learning Analytics and Knowledge,* USA, pp. 4–8, doi: 10.1145/2330601.2330605.

Slade, S., & Prinsloo, P. (2013), "Learning analytics: Ethical issues and dilemmas", *American Behavioral Scientist,* Vol. 57 No. 10, pp. 1510–1529, doi: 10.1177/0002764213479366.

Solove, D. J. (2004), *The digital person: Technology and privacy in the information age*, New York University Press, New York, NY.

Solove, D. J. (2008), *Understanding privacy*, Harvard University Press, Cambridge, MA.

Solove, D. (2013), "Introduction: Privacy self-management and the consent dilemma", *Harvard Law Review,* Vol. 126, pp. 1880–1903, available at: https://harvardlawreview.org/wp-content/uploads/pdfs/vol126_solove.pdf.

Strauss, V. (2018, April 23), "Pearson conducts experiment on thousands of college students without their knowledge", *The Washington Post*, available at: https://www.washingtonpost.com/news/answer-sheet/wp/2018/04/23/pearson-conducts-experiment-on-thousands-of-college-students-without-their-knowledge/.

Syracuse University. (2017), "Library integration in institutional learning analytics (LIILA)", available at: https://www.imls.gov/grants/awarded/lg-98-17-0019-17.

Trustees of Indiana University. (2018), "Getting to know their data doubles: An inquiry into student perceptions of privacy issues associated with academic library participation in learning analytics", available at: https://www.imls.gov/grants/awarded/lg-96-18-0044-18.

University of California. (2017), "University of California: Learning data privacy principles", available at: https://www.ets.berkeley.edu/sites/default/files/general/uc_learning_data_principles_final03.05.2018.pdf.

University of Hawaii. (2018), "20181114 Resolution supporting learning data privacy principles and practices", available at: https://hawaii.edu/uhmfs/public-archive/.

University of Minnesota. (2018), "Unizin Course Monitor aka Snapshot", available at: http://unizin.umn.edu/learning-analytics/unizin-course-monitor-aka-snapshot.

VanScoy, A., & Oakleaf, M. J. (2008), "Evidence vs. anecdote: Using syllabi to plan curriculum-integrated information literacy instruction", *College & Research Libraries*, Vol. 69 No. 6, pp. 566–575, doi: 10.5860/crl.69.6.566.

Vozniuk, A., Govaerts, S., Bollen, L., Manske, S., Hecking, T., & Gillet, D. (2014), "AngeLA: Putting the teacher in control of student privacy in the online classroom", in *Proceedings of Information Technology Based Higher Education and Training (ITHET),* UK, pp. 1–4, doi: 10.1109/ITHET.2014.7155683.

Wasley, P. (2008, March 14), “The syllabus becomes a repository of legalese”, *The Chronicle of Higher Education*, available at: https://www.chronicle.com/article/The-Syllabus-Becomes-a/17723.

Waterhouse, S., & Rogers, R. O. (2004), “The importance of policies in e-learning instruction”, *EDUCAUSE Quarterly,* Vol. 2004 No. 3, pp. 28–39, available at: https://er.educause.edu/~/media/files/article-downloads/eqm0433.pdf.

Williamson, B. (2017), *Big data in education: The digital future of learning, policy and practice*, SAGE Publications, Los Angeles, CA.

Willis, J. E., III, Campbell, J. P., & Pistilli, M. D. (2013), “Ethics, big data and analytics: A model for application”, *EDUCAUSE Review Online*, available at: http://educause.edu/ero/article/ethics-big-data-and-analytics-model-application.

Worthington, B. (2017), “Towards a better understanding of opportunities for performance training within the MLS curriculum: Issues for enhancing education of children's Librarians”, *Journal of Education for Library & Information Science*, Vol. 58 No. 4, pp. 202–218.

Young, J. R. (2018, October 4), “To bring analytics to college classrooms, new effort starts with ‘data laundry’”, *EdSurge*, available at: https://www.edsurge.com/news/2018-10-04-to-bring-analytics-to-college-classrooms-new-effort-starts-with-data-laundry.

Appendices

Appendix A: Codebook

[INSERT TABLE1.docx]